Министерство общего и профессионального образования Ростовской области

государственное бюджетное профессиональное образовательное учреждение Ростовской области

«Ростовский-на-Дону колледж связи и информатики»

(ГБПОУ РО «РКСИ»)

## ОТЧЕТ О ВЫПОЛНЕНИИ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

**по специальности**

**09.02.03 «Программирование в компьютерных системах»**

**Студент Баяндин Иван Владимирович**

*(Фамилия, имя, отчество)*

**Курс 4 Группа ПОКС-47**

|  |  |  |
| --- | --- | --- |
| Общепрофессиональная дисциплина:  ОП.14 «Информационная безопасность» | Преподаватель колледжа:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ О.П. Манакова | |
|  | | Студент:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Ф.И.О. | |

**Ростов-на-Дону**

**2021-2022 уч. г.**

**Практическое занятие №1**

1. Наименование практического занятия: Настройки безопасности и конфиденциальности в браузере.
2. Цели практического занятия: Исследовать настройки безопасности и конфиденциальности в браузере.
3. Количество часов: 2
4. Место проведения: главный корпус РКСИ, ауд. 420.
5. Перечень используемого оборудования: компьютер, выход в глобальную сеть, комплект учебно-методической документации, раздаточный материал, операционная система MS Windows, браузер Google Chrome.
6. Последовательность проведения работ:

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Этап выполнения задания** | Описание выполняемых работ |
| 1 | Очистить кэш и куки в браузере. |  |
| 2 | Найти сайты требующие работу с куки и проверить их работу (скорость загрузки, правильность отображения контента) при отключенных куки в браузере (интернет-магазины, погода и т.п.). | До разрешения использования файлов куки скорость загрузки страницы была низкой, не правильно и не полностью отображался контент. |
| 3 | Выполнить запрет на синхронизацию. |  |
| 4 | Включить режим инкогнито. |  |
| 5 | Вернуть начальные настройки браузера. |  |
| 6 | Проверить наличие цифровых сертификатов, описать назначение 2-3 цифровых сертификатов. | * **Сертификаты, подтверждающие только доменное имя (Domain Validation — DV).** Данный сертификат получается автоматически через центр сертификации. Как следует из названия, такие сертификаты подтверждают только доменное имя. Рядом с адресной строкой для таких сайтов отображается замок белого или серого цвета (в зависимости от браузера), что свидетельствует только о наличии шифрования при передаче данных. * **Сертификаты с валидацией организации (Organization Validation – OV).** Получить подобный сертификат может только компания. Для его выдачи Центр сертификации проверяет: реально ли существует данная организация и принадлежит ли ей конкретный домен. Сайты с данным типом сертификата также отмечаются белым или серым замком рядом с адресной строкой. * **Сертификаты с расширенной проверкой (Extendet Validation – EV).** Самый дорогой и самый сложный в получении вид сертификата. Это обусловлено тем, что для его выдачи центр сертификации проверяет правовую, физическую и операционную деятельность субъекта, а также убеждается, что организация соответствует официальным документам. Помимо этого необходимо убедиться, что компания имеет исключительное право на домен, который указан в сертификате EV. Отличительной особенностью является то, что для сайтов с EV сертификацией рядом с адресной строкой отображается значок зеленого замка. |

7. Контрольные вопросы:

* Всегда ли необходимо отключать файлы куки? Обоснуйте ответ.

Я считаю, что не всегда необходимо отключать файлы куки, т.к. они облегчают взаимодействие с сайтом. Начиная от авторизации, заканчивая сохранением настроек.

* В каких случаях необходимо включать режим инкогнито?

В случае намерения скрыть свои действия в браузере на своём устройстве необходимо включать режим инкогнито

8. Выводы о проделанной работе.

Я исследовал настройки безопасности и конфиденциальности в браузере, а так же попрактиковался.

# Практическое занятие № 2

1. Наименование практического занятия: Защита документов в MS Office.
2. Цели практического занятия: Исследовать возможности настройки защиты документов в MS Office.
3. Количество часов: 2
4. Место проведения: главный корпус РКСИ, ауд. 420.
5. Перечень используемого оборудования: компьютер, выход в глобальную сеть, комплект учебно-методической документации, раздаточный материал, операционная система MS Windows, MS Office.
6. Последовательность проведения работ:

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Этап выполнения задания** | Описание выполняемых работ |
| 1 | 1. В текстовом редакторе MS Word в пункте меню *файл →сведения →защитить документ* реализовать следующие механизмы защиты:    1. Установить пароль на открытие документа.    2. Установить ограничение на редактирование «только чтение» для текущего документа.    3. Определить произвольные фрагменты документа и группы пользователей, которым разрешено их редактирование.    4. Установить защиту на редактирование.    5. Пометить документ как окончательный. |  |
| 2 | 1. В текстовом редакторе MS Excel в пункте меню *файл →сведения →защитить книгу* реализовать следующие механизмы защиты:    1. Установить пароль на открытие документа.    2. Установить защиту на все листы книги, разрешив только выделение ячеек.    3. Выполнить защиту структуры книги.    4. Пометить документ как окончательный. |  |

7. Контрольные вопросы:

1. MS Word. Что подразумевается под опцией «окончательный документ»? Какие действия с ним возможны?

Под «окончательным документом» подразумевается то, что он становится доступным только для чтения, без возможности редактирования.

1. MS Word. Как снять пароль на документе?

Нужно зайти в пункте меню *файл →сведения →защитить документ* и удалить текущий пароль. Нажать кнопку ок.

1. MS Word. В каком случае опция «зашифровать паролем» будет доступна?

Если в открытом файле пароль ещё не задан.

1. MS Word. Как отменить защиту на редактирование областей документа?

*файл →сведения →защитить документ*

Снять ограничения на редактирование

1. MS Excel. Какие действия по защите книги необходимо выполнить, что бы злоумышленник не нарушил ее структуру?

*файл →сведения →защитить книгу и выполнить защиту структуры книги.*

1. MS Excel. Сможет ли защита элементов листа и книги не допустить компрометации книги? Обоснуйте ответ.

Да, защита элементов листа и книги сможет не допустить компрометации книги .

8. Выводы о проделанной работе.

Научился настраивать защиту документов в MS Office

# Практическое занятие № 3

1. Тема практического занятия: Программная реализация алгоритма шифрования и дешифрования информации.
2. Цели практического занятия: Создание программы, реализующей алгоритм шифрования и дешифрования информации.
3. Количество часов: 8
4. Место проведения: главный корпус РКСИ, ауд. 420.
5. Перечень используемого оборудования: компьютер, выход в глобальную сеть, комплект учебно-методической документации, раздаточный материал, операционная система MS Windows, среды программирования.
6. Последовательность проведения работ:

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Этап выполнения задания** | Описание выполняемых работ |
| 1 | Используя знания, умения и навыки, полученные при изучении дисциплины «Технология разработки программного продукта», распределить функции между членами группы, разработать постановку задачи, построить ее блок-схему. | (Группа состоит из 3 человек: Баяндин И.В., Гапонов М.А., Панин А.О.) Программа имеет 2 режима работы, в зависимости от цели (необходимо зашифровать текст, либо дешифровать) |
| 2 | Используя любой язык программирования разработать программный продукт. |  |
| 3 | Произвести его оптимизацию. |  |
| 4 | Произвести отладку программы. |  |
| 5 | Произвести тестирование программы. |  |

7. Контрольные вопросы:

1. Какие языковые конструкции использованы в программе.

Объявление переменных, массивов. Циклы (for), условия (if)

1. Использовались ли процедуры и функции? Описать их назначение

Нет.

1. Используя листинг программы, пояснить работу операторов выполняющих ключевые функции программы.

Шифр состоит их последовательности нескольких шифров Цезаря с различными значениями сдвига. Кириллица состоит из 33 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

8. Выводы о проделанной работе.

Создали программу, реализующую алгоритм шифрования и дешифрования информации.

# Практическое занятие № 4

1. Наименование практического занятия: Система информационной безопасности в организации.
2. Цели практического занятия: Построить систему обеспечения информационной безопасности (СОИБ) условной организации, сформировать последовательность этапов построения СОИБ и перечислить мероприятия, реализуемые на каждом из этапов.
3. Количество часов: 8
4. Место проведения: главный корпус РКСИ, ауд. 420.
5. Перечень используемого оборудования: класс ПК, сеть Интернет, операционная система MS Windows, браузеры, MS Office, индивидуальное задание, конспект лекций, комплект учебно-методической документации, электронные и бумажные методические и справочные материалы.
6. Последовательность проведения работ:

Ход занятия (деятельность студентов):

1. Организовать постоянный состав микрогруппы (ФИО участников заявить преподавателю).
2. Выбрать из предложенного списка организацию для реализации индивидуального задания.
3. Ознакомится с электронными и бумажными методическими и справочными материалами.
4. Реализовать индивидуальное задание в соответствии с поставленными задачами.
5. Оформить полученные результаты в текстовом файле. Сдать на проверку преподавателю.

Список организаций (выбрать одну):

* 1. Салоны красоты.
  2. Автомобили: прокат, аренда.
  3. АЗС.
  4. Выставки.
  5. Строительное оборудование.
  6. Кинотеатры.
  7. Планетарий (дельфинарий).
  8. Туризм.
  9. Торговые базы.
  10. Бытовые услуги.
  11. Изготовление мебели.
  12. Гостиница.
  13. Издательские услуги.
  14. Грузовые перевозки
  15. Провайдеры.

Задачи (для любого индивидуального задания):

1. определить цели и задачи защиты информации в организации;
2. составить матрицу доступа;
3. определить группу требований к автоматизированной системе (АС);
4. определить предмет защиты в организации;
5. выявить возможные угрозы защищаемой информации в организации и их структуру;
6. выявить источники, виды и способы дестабилизирующего воздействия на защищаемую информацию в организации;
7. выявить каналы и методы несанкционированного доступа к защищаемой информации в организации;
8. определить основные направления, методы и средства защиты информации в организации.

При составлении файла необходимо придерживаться следующей структуры отчета:

* 1. Описание организации.
  2. Характеристика информационной системы организации.
  3. Актуальность проблемы защиты информации в организации.
  4. Задачи индивидуального задания.
  5. Цели и задачи защиты информации в организации.
  6. Матрица доступа.
  7. Требования по защите информации от НСД.
  8. Объекты и предмет защиты в организации.
  9. Угрозы защищаемой информации в организации.
  10. Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию в организации.
  11. Каналы и методы несанкционированного доступа к защищаемой информации в организации.
  12. Основные направления, методы и средства защиты информации в организации.
  13. Выводы.

Критерии оценивания результатов практического занятия.

|  |  |
| --- | --- |
| Результат | Критерии |
| Зачет | ставится, если студент выполнил работу в полном объеме с соблюдением необходимой последовательности действий; в ответе правильно и аккуратно выполняет все записи, таблицы, рисунки, чертежи, графики, вычисления; правильно выполняет анализ ошибок. Работа студента характеризуется высокой и средней степенью самостоятельности. Отчет по практическому занятию сдан в установленные сроки. |
| Не зачет | ставится, если студент выполнил работу не полностью, объем выполненной части таков, что не позволяет получить правильные результаты и выводы; в ходе проведения работы были допущены ошибки. Работа студента характеризуется низкой степенью самостоятельности. Отчет по практическому занятию не сдан в установленные сроки. |

7. Контрольные вопросы:

* Какие нормативные документы использовались при построении СОИБ?

ГОСТ Р ИСО 7498-2-99, ГОСТ Р 50739-95, ГОСТ 28147-89.

* Является ли процедура построения СОИБ циклической? Обоснуйте Ваш ответ.

Да, мир и есть цикл.

* Дайте характеристику современным злоумышленникам, совершающим правонарушения в сфере информационной безопасности.

Глупые люди, обладающие некоторым спектром знаний в сфере ИБ, совершающие правонарушения в целях личного обогащения, распространения нелегальной информации, идей терроризма и экстремизма, дискредитации граждан и государств.

* Обоснуйте необходимость проведения регулярной работы с сотрудниками организации.

Необходимо проводить регулярную работу с сотрудниками организации, т.к. постоянно появляются новые средства защиты информации (как и новые софты с противоправным умыслом), улучшения результатов сотрудников в сфере ИБ, возможно получение какой-то обратной информации от сотрудников организации.

* Какова конечная цель полученной СОИБ?

Создание единого комплекса правовых норм, экономических и организационных мер, технических, программных и криптографических средств, а также информационных ресурсов, обеспечивающего минимальные суммарные расходы на предотвращение информационных рисков и компенсацию ущерба от них.

8. Выводы о проделанной работе.

Построили систему обеспечения информационной безопасности (СОИБ) кинотеатра, сформировали последовательность этапов построения СОИБ и перечислили мероприятия, реализуемые на каждом из этапов.